MTHSC 851: Group Theory

1: Groups, Subgroups, & Homomorphisms

Def: A nonempty set with an associative binary operation $*$ is a <u>semigroup</u>.

Def: A semigroup S with an identity elt. 1 s.t. $1x = x1 = x$ $\forall x \in S$ is a <u>monoid</u>.

Def: A <u>group</u> is a monoid G with the property that every $x \in G$ has an inverse $y \in G$ s.t. $xy = yx = 1$.

Prop 1.1 The identity of a monoid is unique.

Pf. Let 1 and e be identity elements. $1 = 1e = e$ $\square$

Prop 1.2 Let G be a group and $x \in G$. Then x has a unique inverse.

Pf. Let y and z be inverses for x.

$$y = y1 = y(xz) = (yx)z = 1 \cdot z = z.$$

Prop 1.3: If G is a group, and $x, y \in G$, then $(xy)^{-1} = y^{-1}x^{-1}$

Pf. $(xy)(y^{-1}x^{-1}) = (x(yy^{-1}))x^{-1} = x1x^{-1} = 1.$

Note: If the binary operation is addition, we write the identity as 0.

Def: G is <u>abelian</u> if $xy = yx$ $\forall x, y \in G$

Fact: $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{mn}$.

Additive analog: $x^n \longleftrightarrow nx$ so

$$mx + nx = (m+n)x \quad \text{and} \quad n(mx) = (mn)x.$$

Pf: Exercise.

Examples of groups

1. $G = \{1, -1\} \subseteq \mathbb{R}$, multiplication
2. $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, addition
3. $G = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, multiplication

   Also for $\mathbb{R}^*$, $\mathbb{C}^*$, but not $\mathbb{Z} \setminus \{0\}$.
4. Let S be a non-empty set. A permutation of S is a bijection $\phi: S \longrightarrow S$.

   Let $G = \mathrm{Perm}(S) = \{\text{permutations of } S\}$.

   Binary operation is composition, i.e.,

   $$[\phi \circ \theta](s) = \phi(\theta(s)).$$

   Associative: $(\phi(\theta\sigma))(s) = \phi(\theta\sigma(s)) = \phi[\theta(\sigma(s))]$.

   and $((\phi\theta)\sigma)(s) = \phi\theta(\sigma(s)) = \phi[\theta(\sigma(s))]$ ✓

   Identity ✓

   Inverse: ✓

5. Special case of Perm(S): let $S = \{1, 2, \ldots, n\}$.
Then Perm(S) is the <u>symmetric group</u>, denoted S_n.

If $\phi \in S_n$, write $\phi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \phi(1) & \phi(2) & \cdots & \phi(n) \end{pmatrix}$

Composition reads right-to-left.

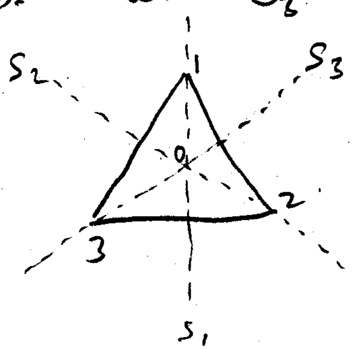
<u>ex:</u> $\phi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\theta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3$

$$\phi\theta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\theta\phi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \phi\theta$$

So S_3 is not abelian.

6. Let $D_3 = \{$symmetries of an equilateral triangle, $T\}$



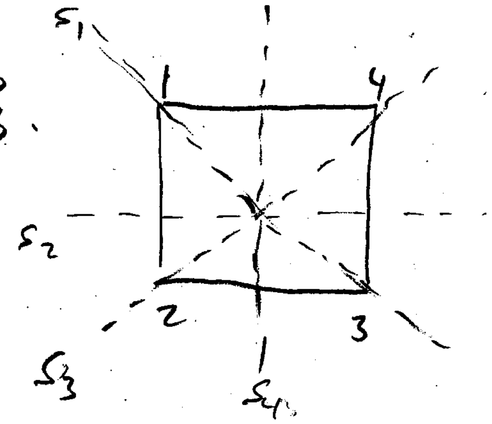
3 rotations: $0°, 120°, 240°$ $(1, r, r^2)$

3 reflections: s_1, s_2, s_3

<u>Exercise:</u>
- Verify this is a group (just need to write out the multiplication table).
- Verify D_3 is "the same" group as S_3.

[4]

7. Let $D_4 = \{\text{symmetries of a square}\}$.



<u>4 rotations</u>: $0, \ 90°, \ 180°, \ 270°$

$\qquad\qquad 1 \quad r \quad r^2 \quad r^3$

<u>4 reflections</u>: s_1, s_2, s_3, s_4

$$D_4 = \{1, r, r^2, r^3, s_1, s_2, s_3, s_4\}$$

<u>Note!</u> Not all permutations are symmetries.

e.g., $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ is not a symmetry.

Therefore, $|S_4| > |D_4|$.

8. Let Q_2 be the <u>quaternion group</u>,

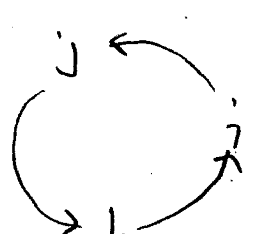
$Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$, where $1 = I_{4\times 4}$,

$$i = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad j = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} \quad k = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Easy to check: $i^2 = j^2 = k^2 = -1$ & $ij = k$.

This determines everything else.

For multiplication think of a cycle: (counterclockwise = positive)



$$\underbrace{\begin{matrix} ij = k \\ jk = i \\ ki = j \end{matrix}}_{\text{ctr-clockwise}} \qquad \underbrace{\begin{matrix} ik = -j \\ kj = -i \\ ji = -k \end{matrix}}_{\text{clockwise}}$$

Why did we introduce Q_2 using matrices?

<u>Ans:</u> Associative law comes for free.

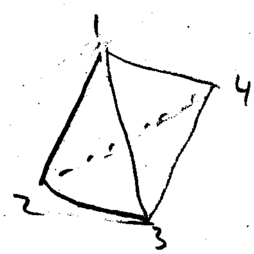
<u>Aside:</u> This is called a <u>representation</u> of Q_2.
(injection into group of matrices).
When a group has a representation, it is a <u>linear group</u>.

<u>Examples of linear groups:</u> Finite groups.
Hyperbolic isometries
Braid groups
Coxeter (reflection) groups

9. Klein 4-group $K = \left\{ \underset{1}{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}, \underset{a}{\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}, \underset{b}{\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}}, \underset{c}{\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}} \right\}$

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

10. Let T be the regular tetrahedron.
Let G = {rotational symmetries}



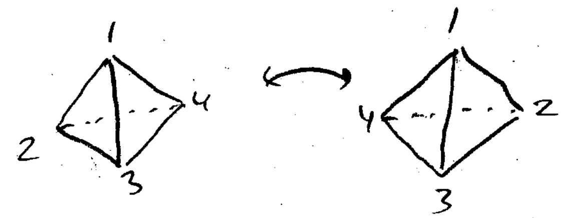
<u>elts of G:</u>

* Identity 1
* (x3) 180° rotations about midpoints of opposite edges
* (x4) 120° rotations that fix one vertex
* (x4) 240° rotations that fix one vertex.

Thus $|G| = 12$.

Let $G^+ = \{\text{symmetries of } T\}$.

G^+ contains G, But we can also take the mirror reflection of T, with each elt of G. This gives us 24 distinct elts.



Note: $|S_4| = 24$, so G^+ and S_4 are the same group.

Def: The cardinality $|G|$ of a group G is its order. If $|G| = \infty$, we say G has infinite order.

Exercise: Check $|S_n| = n!$

Def: A subset $H \subseteq G$ that is a group is called a subgroup of G, and denoted $H \leq G$ or $G \geq H$.

Example: $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

Prop 1.4: If $\emptyset \neq H \subseteq G$, then $H \leq G$ iff $xy^{-1} \in H \; \forall x, y \in H$.

Pf: $\Rightarrow$ ✓

$\Leftarrow$ Show $1 \in H$: Take $x = y$. $x x^{-1} = 1 \in H$ ✓

Show $y^{-1} \in H$ Take $x = 1$. $1 y^{-1} = y^{-1} \in H$ ✓

Show closure: $x(y^{-1})^{-1} = xy \in H$ ✓

$\square$

<u>Cor 1.5</u>: If $\{H_\alpha\}$ is any collection of subgroups of G (not necessarily finite, or countable, etc), then $\bigcap_\alpha H_\alpha \leq G$. $\square$

Let $S \subseteq G$. Consider the set $\bigcap\{H : S \subseteq H \leq G\}$.

- This is a subgroup of G
- It is the smallest subgroup that contains S.

We denote this subgroup by $\langle S \rangle$; it is the subgroup <u>generated by S</u>.

Another way to think of $\langle S \rangle$:

Let $S^{-1} = \{x^{-1} : x \in S\}$

Pick $x_1, x_2, \ldots, x_k \in S \cup S^{-1}$ (for any $k \in \mathbb{N}$, & not necessarily distinct elts).

Consider $\{x_1 x_2 \cdots x_k : x_i \in S \cup S^{-1}, k \in \mathbb{N}\}$. "words in $S \cup S^{-1}$"

This is a subgroup of G. ✓

This is contained in every subgroup that contains H. ✓

Therefore, this must be $\langle S \rangle$.

<u>Def</u>: A group G is cyclic if G is generated by a single element, i.e., $G = \langle x \rangle$.

<u>Example</u>:
- $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$
- Rotation of $\mathbb{R}^2$ by $2\pi/n$ is a cyclic group of order n.

Def: If $x \in G$, define the order of x, denoted $|x|$, to be $|\langle x \rangle|$.

Note: $|x| = \infty$, or $|x| = \min\{n : x^n = 1\}$

Prop 1.6: Suppose $|x| = n < \infty$ and $x^m = 1$. Then $n \mid m$.

Pf: Write $m = nq + r$, $0 \leq r < n$.

Then $1 = x^m = x^{nq+r} = (x^n)^q x^r = x^r \Rightarrow r = 0$. $\square$

Cor: If $G = \langle x \rangle$ of order $n < \infty$, and $k \mid n$, then $\langle x^{n/k} \rangle$ is the unique subgroup of order k in G.

Pf: Clearly, $|x^{n/k}| = k$.

Suppose $|x^s| = k$. Then $x^{sk} = 1 \Rightarrow n \mid sk$

Say $rn = sk$ Then $= (x^{n/k})^r \in \langle x^{n/k} \rangle$.

Thus $\langle x^s \rangle \leq \langle x^{n/k} \rangle$ and $|\langle x^s \rangle| = |\langle x^{n/k} \rangle|$

$\Rightarrow \langle x^s \rangle = \langle x^{n/k} \rangle$. $\square$

Prop 1.7: A subgroup of a cyclic group is cyclic.

Pf: Say $H \leq G = \langle x \rangle$. Suppose $H \neq 1$.

Choose $x^m \in H$ with $m > 0$ minimal.

Claim: $H = \langle x^m \rangle$. Clearly, "$\geq$" holds.

To show "$\leq$", pick $x^k \in H$.

Write $k = mq + r$, $0 \leq r < m$.

$x^k = x^{mq+r} \Rightarrow x^{k-mq} = x^r \in H \Rightarrow r = 0$ by minimality $\square$

Def: If $H \leq G$ and $x, y \in G$, then x & y are <u>congruent mod H</u>, written $x \equiv y \pmod{H}$ if $y^{-1}x \in H$.

<u>Think</u>: "The difference of x & y lies in H"

<u>Exercise</u>: $\equiv$ is an equivalence relation for any H.

<u>Note</u>: $x \equiv y \pmod{H} \iff y^{-1}x = h \in H \iff x = yh$ for $h \in H$.

The equiv. class containing y is $yH := \{yh : h \in H\}$, called the <u>left coset of H</u> containing y.

<u>Note</u>: $xH = yH$ (as sets) iff $x \equiv y \pmod{H}$.

<u>Def</u>: The <u>index</u> of H in G = # distinct left cosets of H in G, and denoted $[G:H]$.

<u>Thm 1.8</u> (Lagrange): If $|G| < \infty$ and $H \leq G$, then
$$|G| = [G:H]\,|H| \qquad (\text{So in particular, } |H| \mid |G|.)$$

<u>Pf</u>: The map $H \longrightarrow xH$, $h \longmapsto xh$ is a bijection. (check!)
Therefore, $|xH| = |yH|$ $\forall x, y \in G$.
Since G is a disjoint union of left cosets of H, & there are $[G:H]$ left cosets of H, $|G| = [G:H] \cdot |H|$. $\square$

Def: A homomorphism f: from G to H is a function $f: G \to H$ such that $f(xy) = f(x)\, g(y)$.

If f is 1-1, it is a monomorphism
If f is onto, it is an epimorphism.

If f is 1-1 & onto, it is an isomorphism; G & H are isomorphic, written $G \cong H$.

A homomorphism $f: G \to G$ is an endomorphism
An isomorphism $f: G \to G$ is an automorphism.

The kernel of a homomorphism $f: G \to H$ is the set
$$\ker f = \{x \in G : f(x) = 1\}$$

Prop 1.9: If $f: G \to H$ is a homom, then $\ker f \leq G$, and f is a monom iff $\ker f = 1$.

Pf: $f(1) = f(1 \cdot 1) = f(1)\, f(1) \implies \boxed{f(1) = 1}$

$1 = f(1) = f(x x^{-1}) = f(x)\, f(x^{-1}) = 1 \implies \boxed{f(x)^{-1} = f(x^{-1})}$

Now, we must show that if $x, y \in \ker f$, $xy^{-1} \in \ker f$.

$f(xy^{-1}) = f(x)\, f(y^{-1}) = f(x)\, f(y)^{-1} = 1 \cdot 1 = 1$ ✓

Therefore, $\ker f \leq G$.

Next, note that
$$f(x) = f(y) \iff f(x)\, f(y)^{-1} = f(xy^{-1}) = 1 \iff xy^{-1} \in \ker f$$

f monom $\implies \ker f = 1$ ✓

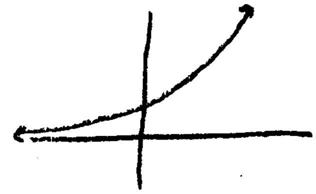
Suppose $\ker f = 1$. Must show $f(x) = f(y) \implies x = y$.

$f(x) = f(y) \implies f(xy^{-1}) = 1 \implies xy^{-1} = 1 \implies x = y$ ✓

$\square$.

Examples:

11. Let $G = (\mathbb{R}, +)$. $H = \{r \in \mathbb{R} : r > 0\}$



$f : G \longrightarrow H$, $f(r) = e^r$ is an isomorphism

$f^{-1} : H \longrightarrow G$, $f^{-1}(x) = \ln x$

Check: $f(r+s) = e^{r+s} = e^r e^s = f(r) f(s)$.

Note: $f(0) = e^0 = 1$. So $id = 0$ in G, but $id = 1$ in H.

12. Let $G = Sym(\Delta)$, $H = \{\pm 1\}$

Define $f(\phi) = \begin{cases} 1 & \phi \text{ is a rotation} \\ -1 & \phi \text{ is a reflection} \end{cases}$

f is a homom. (check!)

13. Let G be abelian, $n \in \mathbb{Z}$.

$f : G \longrightarrow G$, $f(x) = x^n$ is an endomorphism, since $(xy)^n = x^n y^n$.

14. Let $G = S_3$, $H = \mathbb{Z}_6$. $G \not\cong H$, since H is abelian, G is not.

Prop 1.10: If G is a group, then $\operatorname{Aut} G$ is a group w.r.t. composition.

Pf: Pick $f, g \in \operatorname{Aut} G$. Must show $fg^{-1} \in \operatorname{Aut} G$.

$$(fg^{-1})(xy) = f(g^{-1}(xy)) = f(g^{-1}(x) g^{-1}(y)) = f(g^{-1}(x)) f(g^{-1}(y))$$
$$= fg^{-1}(x)\, fg^{-1}(y).$$

$\Rightarrow fg^{-1}$ is a homom, & is in $Perm(G)$, so $fg^{-1} \in \operatorname{Aut} G$, which is a group. $\square$

Def: Let $H \leq G$. Then H is <u>normal</u> in G (or a "normal subgroup of G") if $x^{-1}Hx \subseteq H$ for all $x \in G$.

Since $|x^{-1}Hx| = H$, if $x^{-1}Hx \subseteq H$, then $x^{-1}Hx = H$.

We write this as $H \triangleleft G$, or $G \triangleright H$.

<u>Exercise</u>: If $H \leq G$, then $H \triangleleft G$ iff every right coset is a left coset.

<u>Prop</u>: Let $f : G \to H$ be a homom, & set $K = \ker f$. Then $K \triangleleft G$.

<u>Pf</u>: Need to show that $xkx^{-1} \in K$ for all $x \in G$,

i.e., that $f(xkx^{-1}) = 1$.

$$f(xkx^{-1}) = f(x)f(k)f(x)^{-1} = f(x) \cdot 1 \cdot f(x)^{-1} = 1 \quad \checkmark \qquad \square$$

<u>Def</u>: The <u>center</u> of G is the set

$$Z(G) = \{ x \in G : xy = yx \text{ for all } y \in G \}$$

i.e., "elements that commute with everything in G."

<u>Exercise</u>: Show $Z(G) \triangleleft G$.

<u>Recall</u>: We defined $\equiv$ mod $H \leq G$ as

$$x \equiv y \bmod H \Rightarrow y^{-1}x \in H \Rightarrow y^{-1}xH = H \Rightarrow xH = yH$$

We could have instead defined it as

$$x \equiv y \bmod H \Rightarrow xy^{-1} \in H \Rightarrow Hxy^{-1} = H \Rightarrow Hx = Hy.$$

here, the equivalence classes are the <u>right cosets</u> of H in G.

* Big idea of normal subgroups:

If $N \triangleleft G$, then there is a well-defined quotient group G/N.

<u>Q</u>: What does it mean for a map to be well-defined?

<u>A</u>: If $x = y$ (or $x \equiv y$, $x \sim y$, etc), then $f(x) = f(y)$.

If $H \trianglelefteq G$, write G/H for the set of cosets of H in G.

<u>Note</u>: $|G/H| = [G:H]$ and $|G/H| = |G|/|H|$.

If $xH, yH \in G/H$, define a product by $(xH)(yH) = xyH$.

<u>Check well-defined</u>: Suppose $xH = uH$, $yH = vH$.

Since $H \trianglelefteq G$, $xH = Hx$, $yH = Hy$.

so $(xH)(yH) = xyH = xHy = uHy = uyH = uvH = (uH)(vH)$.

<u>Check</u>: G/H is a group, with identity $1H = H$.

This is the <u>quotient group</u> of G mod H.

The map $\eta : G \longrightarrow G/H$, $\eta : x \longmapsto xH$ is the <u>canonical quotient map</u>. Note: $\ker \eta = H$.

<u>Note</u>: If G is written additively, write cosets as $x + H$, and $(x+H) + (y+H) = (x+y) + H$.

<u>Example</u>: let $G = \mathbb{Z}$, $H = n\mathbb{Z}$.

$G/H = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$, where $\bar{k} = k + n\mathbb{Z}$.

Denote this as $G/H = \mathbb{Z}_n = \langle \bar{1} \rangle$

Thm 1.1: (Fundamental Homomorphism Theorem).

Let $f: G \twoheadrightarrow H$ be a (surj.) homom, and let $K = \ker f$.
Then $K \trianglelefteq G$ and $G/K \cong H$.

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\eta"'] & & H \\ & G/K \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd}$$

Pf: Show that there is an isomorphism $\bar{f}: G/K \to H$ such that $\bar{f}\eta = f$.

Define $\bar{f}(xK) = f(x)$.

$$\begin{tikzcd} x \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\eta"'] & & f(x) \\ & xK \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd}$$

<u>Check well-defined</u>

Suppose $xK = yK$. Then $y^{-1}x \in K$.
$1 = f(y^{-1}x) = f(y^{-1})f(x) = f(y)^{-1}f(x) = 1 \Rightarrow f(x) = f(y)$ ✓

<u>Check homom</u>

$\bar{f}(xKyK) = \bar{f}(xyK) = f(xy) = f(x)f(y) = \bar{f}(xK)\bar{f}(yK)$. ✓

<u>Check injective:</u>

$\bar{f}(xK) = \bar{f}(yK) \Rightarrow f(x) = f(y) \Rightarrow f(y)^{-1}f(x) = 1$
$\Rightarrow f(y^{-1}x) = 1 \Rightarrow y^{-1}x \in K \Rightarrow y^{-1}xK = K \Rightarrow xK = yK$. ✓

(alternatively, $\ker \bar{f} = \{xK : f(x) = 1\} = \{xK : x \in K\} = K$)

<u>Check surjective</u> Immediate, since f is surj.

Thus, $\bar{f}: G/K \to H$ is an isomorphism. $\square$

Prop 1.12: (Correspondence thm): Let $N \trianglelefteq G$. There is a bijection: $\{A : N \leq A \leq G\} \longleftrightarrow \{\bar{A} \leq G/N\}$.

"The structure of the subgroups of G/N is the same as the structure of the subgroups of G containing N, with N collapsed to the id. (i.e, mod N)"

$$\begin{tikzcd} G \arrow[r] \arrow[d, dash] & G/N \arrow[d, dash] \\ A \arrow[r] \arrow[d, dash] & A/N \arrow[d, dash] \\ N \arrow[r] & 1 \end{tikzcd}$$

Pf: Show the map $\theta: A \longmapsto A/N$ is a bijection.

1-1: Suppose $A/N = B/N$. Then for any $a \in A$, $aN = bN$ for some $b \in B$.

$\Rightarrow b^{-1}a \in N \subseteq B \Rightarrow a \in B \Rightarrow A \subseteq B$.

Similarly, $B \subseteq A$.

onto: Suppose $\bar{A} \leq G/N$. Define $A = \{x \in G : xN \in \bar{A}\}$.

Check: $A \leq G$, and $\theta(A) = \bar{A}$. $\square$

Exercise: $\bar{A} \trianglelefteq G/N \iff A \trianglelefteq G$.

Thm 1.13: (Freshman Thm). Suppose $K \trianglelefteq H \trianglelefteq G$ and $K \trianglelefteq G$.

Then $H/K \trianglelefteq G/K$ and $G/H \cong (G/K)/(H/K)$.

Pf: Define $f: G/K \longrightarrow G/H$, $f(xK) = xH$.

Show f is a homom, and $\ker f = H/K$.

well-defined: Say $xK = yK$. Then $xKH = yKH = xH = yH$. ✓

homom: $f(xK\,yK) = f(xyK) = xyH = xHyH = f(xK)f(yK)$ ✓

$\ker f = \{xK : xH = H\} = \{xK : x \in H\} = H/K$. Apply Thm 1.11 (FHT) $\square$